

UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF CALIFORNIA
SAN JOSE DIVISION

CHASOM BROWN, et al.,
Plaintiffs,
v.
GOOGLE LLC,
Defendant.

Case No. 20-CV-03664-LHK

**ORDER DENYING MOTION TO
DISMISS**

Re: Dkt. No. 164

Plaintiffs Chasom Brown, William Byatt, Jeremy Davis, Christopher Castillo, and Monique Trujillo (collectively, “Plaintiffs”), individually and on behalf of all others similarly situated, bring the instant case against Defendant Google LLC (“Google”). Plaintiffs’ Second Amended Complaint asserts seven claims against Google under federal and California law. ECF No. 136-1 (“SAC”). Before the Court is Google’s motion to dismiss two of those claims. ECF No. 164.¹ Having considered the parties’ submissions, the relevant law, and the record in this case, the Court DENIES Google’s motion to dismiss.

¹ Google’s motion to dismiss contains a notice of motion that is separately paginated from the points and authorities in support of the motion. Civil Local Rule 7-2(b) requires that the notice of motion and the points and authorities in support of the motion be contained in one document with the same pagination for a total of no more than 25 pages. *See* Civ. Loc. R. 7-2(b).

I. BACKGROUND

To access a website on the internet, an individual must use “web-browsing software” (a “browser”). *See* SAC ¶¶ 2, 63. Specifically, the user must type the website’s Uniform Resource Locator (“URL”) into the browser’s address bar. *Id.* ¶ 63. Entering a URL causes the browser to send a “GET request” to the website’s server. *Id.* A GET request tells the server “what information is being requested” and instructs the server “to send the information back.” *Id.* The browser then displays the requested information for the user. *Id.*

Google provides services and products both to website publishers and to internet users. Google provides advertising and data analytics services to website publishers. *See id.* ¶¶ 8, 67–83. More than 70% of website publishers in the United States use at least one of these services. *Id.* ¶ 8. Google provides internet users with a browser called “Google Chrome” (“Chrome”). *See id.* ¶ 51. Chrome, like other popular browsers, offers a “private browsing mode.” *Id.* ¶ 52. Chrome’s “private browsing mode” is called “Incognito Mode.” *Id.*

The instant case arises from Google’s practice of using its advertising and data analytics services to collect data from internet users who visit websites while in “private browsing mode.” *See id.* ¶¶ 5, 8. Plaintiffs are Google account holders “whose internet use was tracked by Google . . . while browsing the internet from a browser in a private browsing mode.” *Id.* ¶ 11. Specifically, each Plaintiff “visited several major websites using Chrome, in Incognito Mode,” and Google “tracked . . . and intercepted [their] communications with [those] Websites.” *See id.* ¶¶ 168–69, 173–74, 178–79, 183–84, 188–89. Plaintiffs allege that Google’s data collection practice was unlawful because, among other reasons, Google represented that using “private browsing mode” would prevent Google from collecting Plaintiffs’ data. *Id.* ¶ 6.

In the following sections, the Court describes in turn: (1) Google’s practice of collecting the data of internet users who visit Google affiliated websites; (2) Google’s representations regarding “private browsing mode”; and (3) the procedural history of the instant case.

A. Google’s Data Collection Practices

Plaintiffs provide detailed allegations explaining how Google collects and monetizes

internet users' data. The Court begins by describing Google's techniques for collecting internet users' data. The Court then describes how Google monetizes that data.

1. Google's Techniques for Collecting Data

Google offers two services that are used by more than 70% of websites: Google Analytics and Google Ad Manager. *See* SAC ¶ 63. Google Analytics enables a website publisher to collect information "about the origins of [the] Website's traffic, demographics, frequency, browsing habits on the Website, and other data about visitors." *Id.* ¶ 67. Although the basic version of Google Analytics is free, publishers may pay for "more specific and granular data about visitors." *Id.* ¶ 67 n.17. In turn, Google Ad Manager enables a website publisher to "display targeted Google advertisements . . . along with the Website's actual content." *Id.* ¶ 79. "Google's advertising customers" pay fees to display these advertisements, and the fees are split between Google and the website publisher. *Id.* To use Google Analytics and Google Ad Manager, publishers must "embed" customized Google code into their websites' code. *See id.* ¶¶ 68, 79.

According to Plaintiffs, Google collects the data of all internet users who visit websites that use Google Analytics and Google Ad Manager. As discussed, an internet user accesses a website by causing a browser to send a "GET request" to the server that contains the website's information. *Id.* ¶ 63. When a browser sends a GET request to a website that uses either Google Analytics or Google Ad Manager, the embedded Google code causes the browser to send a duplicate GET request directly to Google. *Id.* Because the GET request describes "what information is being requested" by the browser, obtaining the duplicate GET request "enables Google to learn exactly what content the [browser] was asking the website to display." *Id.* The duplicate GET request also includes the "URL information of what the user has been viewing and requesting from websites online." *Id.*

Additionally, every website that uses Google Analytics or Google Ad Manager collects each visitor's Internet Protocol ("IP") address. *Id.* An IP address is a unique identifier that an Internet Service Provider ("ISP") assigns to a device when the device uses an internet connection provided by the ISP. *See id.* ¶ 63 n.16. Because most internet users access the internet using one

1 device and one internet connection, most internet users have one IP address. *Id.* ¶ 63 n.16. Thus,
2 obtaining an internet user’s IP address allows Google to track that user across the internet.

3 Google also uses “cookies” and “pixels” to obtain data. As a user browses the internet, the
4 user’s browser records “cookies,” which are “piece[s] of code” that contain “information
5 regarding the state of the user’s system . . . or information regarding the user’s browsing activity.”
6 *Id.* ¶ 70 n.19. When a user visits a website that has Google Analytics or Google Ad Manager, the
7 embedded Google code causes the browser to send Google cookies that contain information about
8 “the prior websites the user has viewed.” *Id.* ¶ 70. The embedded Google code also causes the
9 browser to display a “digital pixel.” *Id.* ¶ 102. This function allows Google to differentiate
10 between users because “digital pixels . . . display differently for every device and application.”
11 *Id.* ¶ 100. Thus, “[b]y tracking these pixels and the unique resulting displays, Google and its . . .
12 partners are able to track and ‘measure’ [users] across the web.” *Id.* ¶ 103.

13 Website publishers that use Google Analytics may pay “additional fees” for a feature
14 called “Google Analytics User-ID.” *Id.* ¶ 69. This feature “allows Websites to ‘generate [their]
15 own unique IDs, consistently assigns IDs to users, and include these IDs wherever [the Websites]
16 send data to Analytics.” *Id.* (alterations in original). These IDs are more useful to websites than
17 IP addresses because a user’s ID stays the same when the user accesses the website from different
18 devices. *Id.* Thus, the “‘same search on a phone, purchases on a laptop, and re-engagement on a
19 tablet that previously looked like three unrelated actions on unrelated devices can now be
20 understood as one user’s interactions with [the website’s] business.’” *Id.* (alteration in original).

21 Google can collect additional data if a user accesses the internet with certain Google
22 software applications. Most importantly, when a user installs Chrome on a device, Google assigns
23 the device a “unique digital string of characters called Google’s ‘X-Client-Data Header.’” *Id.*
24 ¶ 95. Then, whenever the user accesses Google affiliated websites with Chrome, Google will
25 receive the user’s “X-Client-Data Header.” *Id.* ¶ 98. Additionally, if a user has a cellular device
26 with Google’s Android operating system or any of Google’s mobile applications, the device will
27 “constantly send[] system and location data to Google.” *Id.* ¶ 106.

Generally, Google collects a user’s data regardless of whether the “user . . . enters ‘private browsing mode’ on the user’s browser software.” *Id.* ¶ 84. However, Google does not receive a Chrome user’s “X-Client-Data Header” if the user enters “Incognito Mode.” *Id.* ¶ 98.

2. Google’s Monetization of Data

Google monetizes internet users’ data by “creat[ing] ‘profiles’ for each individual user and/or each individual device that accesses the Internet.” *Id.* ¶ 116. Website publishers purchase these profiles from Google to learn about the browsing habits of the users who visit the publishers’ websites. *Id.* ¶¶ 116–17. Google also uses these profiles to create “targeted advertisements” for “third-party advertisers.” *See id.* ¶¶ 118–19. Specifically, the Google Ad Manager service, which is used by more than 70% of websites, receives the profiles of individuals who visit those websites and uses algorithms to determine which advertisements to show to those individuals. *Id.* Google demands “high prices for these targeted-advertising services.” *Id.*

According to Plaintiffs, the data that Google collects from internet users is “viewed as a form of currency” in the “e-commerce industry.” *Id.* ¶ 123. Indeed, the “cash value” of this data “can be quantified.” *Id.* ¶ 127. For example, a study of “180 internet users” found that users are willing to pay \$52.00/year to keep their browsing histories private. *Id.* ¶ 128. Similarly, Google itself has set up a project called “Google Screenwise Trends” which pays internet users to “add a browser extension that shares with Google the sites they visit and how they use them.” *Id.* ¶ 129. Google pays participants “up to \$3 *per week* to be tracked.” *Id.* ¶ 130 (emphasis in original).

Indeed, “a number of platforms have appeared where consumers can and do directly monetize their own data.” *Id.* ¶ 135. For example, a company called Brave now offers a web browser which “will pay users to watch online targeted ads, while blocking out everything else.” *Id.* Several other companies have launched exchange platforms that allow internet users to sell their data to applications and websites. *See id.*

B. Google’s Representations Regarding “Private Browsing Mode”

Plaintiffs allege that Google made numerous representations that, if Plaintiffs visited websites while in “private browsing mode,” Google would not collect their data. Specifically,

Plaintiffs identify three Google documents that contain privacy-related representations: (1) Google’s Privacy Policy; (2) Chrome’s Privacy Notice; and (3) the “Incognito Splash Screen.” The Court discusses each document in turn.

1. Google’s Privacy Policy

The “Introduction” section of Google’s Privacy Policy informs internet users that they can “choose to browse the web privately using Chrome in Incognito mode.” SAC ¶ 45. The following sentence adds: “across [Google’s] services, you can adjust your privacy settings to control what [Google] collect[s] and how your information is used.” *Id.*

To help users adjust their privacy settings, Google’s Privacy Policy includes a section called “Your privacy controls.” *Id.* ¶ 46. The “Your privacy controls” section states that users “have choices regarding the information [Google] collect[s] and how it’s used.” *Id.*

Additionally, the “Your privacy controls” section contains links to two pages that encourage users to enter “private browsing mode”: (1) the “Search & Browse Privately” page and (2) the “See & control your Web & App Activity” page. The “Search & Browse Privately” page reiterates that users are “in control” of their information and states that, to control their information, users can “enabl[e] ‘private browsing mode’ on their browsers,” which will “allow [users] to ‘browse the web privately.’” *Id.* ¶ 48. In turn, the “See & control your Web & App Activity” page informs users that “search and ad results may be customized using search-related activity even if you’re signed out.” *Id.* ¶ 49. However, the page also states that a user can “turn off this kind of search customization” by “search[ing] and brows[ing] privately” and provides a link to “Learn how.” *Id.* Clicking on “Learn how” takes the user to the “Search & Browse Privately” page which, as noted, encourages users to “enabl[e] ‘private browsing mode.’” *Id.*

2. Chrome Privacy Notice

The purpose of the Chrome Privacy Notice is to inform Chrome users “how to control the information that’s collected, stored, and shared when [they] use the Google Chrome browser.” ECF No. 165-22 at 1. The Chrome Privacy Notice directly incorporates Google’s Privacy Policy and explains that “any personal information that is provided to Google or stored in your Google

Account will be used and protected in accordance with the Google Privacy Policy.” *See id.*

Additionally, the Chrome Privacy Notice lists the various “browser modes” that are available in Chrome and states that “[p]rivacy practices are different depending on the mode that you’re using.” *Id.* at 3. Under the section labeled “Incognito mode and guest mode,” the Chrome Privacy Notice states: “You can limit the information Chrome stores on your system by using incognito mode or guest mode.” *Id.* at 11. The phrase “incognito mode or guest mode” has a hyperlink which directs users to a page titled “Browse in private.” *Id.* The “Browse in private” page provides instructions on how to open Chrome in Incognito Mode from any device. *Id.*

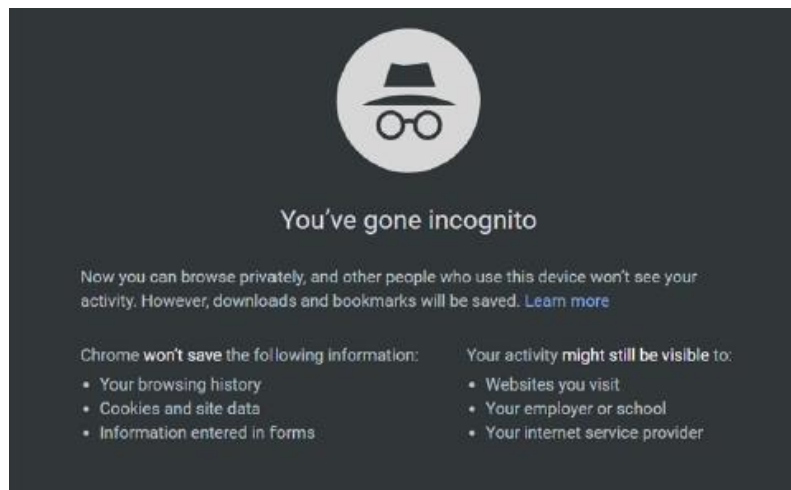
The Chrome Privacy Notice further states that, when Chrome is in Incognito Mode, “Chrome won’t store certain information, such as”:

- Basic browsing history information like URLs, cached page text, or IP addresses of pages linked from the websites you visit;
- Snapshots of pages that you visit; and
- Records of your downloads, although the files you download will still be stored elsewhere on your computer or device.

Id. Additionally, the Chrome Privacy Notice states that “Chrome won’t share existing cookies with sites you visit in incognito or guest mode.” *Id.*

3. “Incognito Splash Screen”

When a user opens Chrome in Incognito Mode, Chrome displays the following message:



1 SAC ¶ 52. Plaintiffs refer to this display as the “Incognito Splash Screen.” *See* ECF No. 192 at 5.

2 **C. Procedural History**

3 On June 2, 2020, Plaintiffs filed a complaint against Alphabet, Inc. (“Alphabet”) and
4 Google alleging that Google had unlawfully collected Plaintiffs’ data while Plaintiffs used
5 “private browsing mode.” ECF No. 1. Plaintiffs asserted four claims: (1) unauthorized
6 interception under the Wiretap Act, 18 U.S.C. § 2510 *et seq.*; (2) violation of the California
7 Invasion of Privacy Act (“CIPA”), Cal. Penal Code §§ 631 and 632; (3) invasion of privacy; and
8 (4) intrusion upon seclusion. *Id.*

9 Additionally, the complaint sought class action relief on behalf of two alleged classes: (1)
10 “All Android device owners who accessed a website containing Google Analytics or Ad Manager
11 using such a device and who were (a) in ‘private browsing mode’ on that device’s browser and (b)
12 were not logged into their Google account on that device’s browser, but whose communications,
13 including identifying information and online browsing history, Google nevertheless intercepted,
14 received, or collected from June 1, 2016 through the present” and (2) “All individuals with a
15 Google account who accessed a website containing Google Analytics or Ad Manager using any
16 non-Android device and who were (a) in ‘private browsing mode’ in that device’s browser, and (b)
17 were not logged into their Google account on that device’s browser, but whose communications,
18 including identifying information and online browsing history, Google nevertheless intercepted,
19 received, or collected from June 1, 2016 through the present.” *Id.* ¶ 95.

20 On August 20, 2020, Plaintiffs and Alphabet stipulated to dismiss Alphabet from the case
21 without prejudice. ECF No. 51. On the same day, Google filed a motion to dismiss the complaint.
22 ECF No. 53. On August 24, 2020, the Court granted the parties’ stipulation to dismiss Alphabet,
23 leaving Google as the only defendant. ECF No. 57.

24 On September 21, 2020, Plaintiffs filed a first amended complaint (“FAC”) in lieu of
25 opposing the motion to dismiss. ECF No. 68 (“FAC”). In addition to the four claims from the
26 original complaint, the FAC asserted a claim for violation of the California Computer Data Access
27 and Fraud Act (“CDAFA”), Cal. Penal Code § 502. *Id.* On October 6, 2020, the Court denied as
28

moot the August 20, 2020 motion to dismiss. ECF No. 74.

On October 21, 2020, Google filed a motion to dismiss the FAC. ECF No. 82. Among other arguments, Google argued that all of Plaintiffs' claims should be dismissed because Plaintiffs consented to Google's collection of Plaintiffs' data. *Id.* at 9–13. In connection with its motion to dismiss, Google filed a request for judicial notice. ECF No. 84. Specifically, Google requested that the Court take notice of twenty-seven documents, including Google's Terms of Service, fifteen versions of Google's Privacy Policy, two versions of Google's Chrome Privacy Notice, and nine publicly available Google webpages. *Id.*

On November 18, 2020, Plaintiffs filed an opposition to Google's motion to dismiss the FAC. ECF No. 87. In connection with their opposition, Plaintiffs filed a response to Google's request for judicial notice, ECF No. 88, and filed their own request for judicial notice, ECF No. 89. Specifically, Plaintiffs requested that the Court take notice of Google's Privacy Policy in effect between March 31, 2020 and July 1, 2020. ECF No. 89.

On December 7, 2020, Google filed a reply in support of its motion to dismiss the FAC, ECF No. 92 ("Reply"), and a filed reply in support of its request for judicial notice, ECF No. 93.

On February 25, 2021, the Court held a hearing on Google's motion to dismiss the FAC. ECF No. 103. At that hearing, Google raised for the first time arguments regarding the Court's website. *See* Tr. of Feb. 25, 2021 Hearing at 47:13–16, ECF No. 104. On February 26, 2021 and March 1, 2021, Google filed affidavits further explaining the arguments regarding the Court's website. ECF Nos. 106, 107. On March 8, 2021, Plaintiffs filed a response addressing the arguments raised in Google's affidavits. ECF No. 111. On March 11, 2021, Google filed an administrative motion for leave to file a reply in support of the arguments raised in Google's affidavits. ECF No. 112.

On March 12, 2021, the Court issued an order granting both parties' requests for judicial notice, denying Google's administrative motion for leave to file a reply in support of the arguments raised in Google's affidavits, and denying Google's motion to dismiss the FAC. *Brown v. Google LLC*, 525 F. Supp. 3d 1049 (N.D. Cal. 2021). Among other holdings, the Court held

that Google failed to show that Plaintiffs consented to Google’s data collection practices. *Id.* at 1064. The Court explained that “Google’s representations regarding private browsing present private browsing as a way that users can manage their privacy and omit Google as an entity that can view users’ activity while in private browsing mode.” *Id.*

On April 14, 2021, the parties stipulated to allow Plaintiffs to file a second amended complaint (“SAC”). ECF No. 136. In addition to the five claims asserted by the FAC, the SAC asserts two new claims against Google: (1) breach of contract; and (2) violation of the California Unfair Competition Law (“UCL”), Cal. Bus. & Prof. Code §§ 17200, *et seq.* ECF No. 136-1 (“SAC”). On April 15, 2021, the Court granted the parties’ stipulation. ECF No. 138.

On May 17, 2021, Google filed a motion to dismiss Plaintiffs’ claims for breach of contract and violation of the UCL. ECF No. 165 (“Mot.”). In connection with its motion to dismiss, Google filed a request for judicial notice. ECF No. 166.

On June 15, 2021, Plaintiffs filed an opposition to Google’s motion to dismiss Plaintiffs’ claims for breach of contract and violation of the UCL. ECF No. 192 (“Opp.”). In connection with their opposition, Plaintiffs filed a request for judicial notice. ECF No. 193.

On June 29, 2021, Google filed a reply in support of its motion to dismiss Plaintiffs’ claims for breach of contract and violation of the UCL. ECF No. 208 (“Reply”).

II. REQUESTS FOR JUDICIAL NOTICE

Google requests that the Court take judicial notice of twenty-four documents, which include three versions of Google’s Terms of Service, sixteen versions of Google’s Privacy Policy, three versions of Google’s Chrome Privacy Notice, and two publicly available Google webpages. ECF No. 166. Plaintiffs request that the Court take judicial notice of the current version of Google’s Chrome Privacy Notice. ECF No. 193.

As the Court previously has explained, these documents appear on publicly available websites and are thus proper subjects of judicial notice. *See Brown*, 525 F. Supp. 3d at 1061 (taking judicial notice of Google’s Terms of Service, Privacy Policy, Chrome Privacy Notice, and webpages); *see also, e.g., In re Google Assistant Privacy Litig.*, 457 F. Supp. 3d 797, 813–14

(N.D. Cal. 2020) (taking judicial notice of Google’s Terms of Service, Privacy Policy, and a Google blog post); *Matera v. Google, Inc.*, 2016 WL 5339806, at *7 (N.D. Cal. Sept. 23, 2016) (taking judicial notice of Google’s Terms of Service, “various versions of Google’s Privacy Policy,” and a Google webpage entitled “Updates: Privacy Policy”).

III. LEGAL STANDARD

A. Motion to Dismiss Under Rule 12(b)(6)

Rule 8(a) of the Federal Rules of Civil Procedure requires a complaint to include “a short and plain statement of the claim showing that the pleader is entitled to relief.” Fed. R. Civ. P. 8(a). A complaint that fails to meet this standard may be dismissed pursuant to Federal Rule of Civil Procedure 12(b)(6). Rule 8(a) requires a plaintiff to plead “enough facts to state a claim to relief that is plausible on its face.” *Bell Atlantic Corp. v. Twombly*, 550 U.S. 544, 570 (2007). “A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged.” *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009). “The plausibility standard is not akin to a probability requirement, but it asks for more than a sheer possibility that a defendant has acted unlawfully.” *Id.* (internal quotation marks omitted). For purposes of ruling on a Rule 12(b)(6) motion, the Court “accept[s] factual allegations in the complaint as true and construe[s] the pleadings in the light most favorable to the nonmoving party.” *Manzarek v. St. Paul Fire & Marine Ins. Co.*, 519 F.3d 1025, 1031 (9th Cir. 2008).

The Court, however, need not accept as true allegations contradicted by judicially noticeable facts, *see Shwarz v. United States*, 234 F.3d 428, 435 (9th Cir. 2000), and it “may look beyond the plaintiff’s complaint to matters of public record” without converting the Rule 12(b)(6) motion into a motion for summary judgment, *Shaw v. Hahn*, 56 F.3d 1128, 1129 n.1 (9th Cir. 1995). Nor must the Court “assume the truth of legal conclusions merely because they are cast in the form of factual allegations.” *Fayer v. Vaughn*, 649 F.3d 1061, 1064 (9th Cir. 2011) (per curiam) (quoting *W. Mining Council v. Watt*, 643 F.2d 618, 624 (9th Cir. 1981)). Mere “conclusory allegations of law and unwarranted inferences are insufficient to defeat a motion to

dismiss.” *Adams v. Johnson*, 355 F.3d 1179, 1183 (9th Cir. 2004).

B. Leave to Amend

If the Court determines that a complaint should be dismissed, it must then decide whether to grant leave to amend. Under Rule 15(a) of the Federal Rules of Civil Procedure, leave to amend “shall be freely given when justice so requires,” bearing in mind “the underlying purpose of Rule 15 to facilitate decisions on the merits, rather than on the pleadings or technicalities.” *Lopez v. Smith*, 203 F.3d 1122, 1127 (9th Cir. 2000) (en banc) (alterations and internal quotation marks omitted). When dismissing a complaint for failure to state a claim, “a district court should grant leave to amend even if no request to amend the pleading was made, unless it determines that the pleading could not possibly be cured by the allegation of other facts.” *Id.* at 1130 (internal quotation marks omitted). Accordingly, leave to amend generally shall be denied only if allowing amendment would unduly prejudice the opposing party, cause undue delay, or be futile, or if the moving party has acted in bad faith. *Leadsinger, Inc. v. BMG Music Publ’g*, 512 F.3d 522, 532 (9th Cir. 2008).

IV. DISCUSSION

Google moves to dismiss Plaintiffs’ breach of contract claim and UCL claim. *See* Mot. at 4, 16. The Court begins with Google’s arguments regarding Plaintiffs’ breach of contract claim and then discusses Google’s arguments regarding Plaintiffs’ UCL claim.

A. Plaintiffs Have Adequately Stated a Breach of Contract Claim Based on Google’s Data Collection Practice

“The elements for breach of contract under California law are: (i) the existence of a contract; (ii) the plaintiff’s performance or excuse for nonperformance of its side of the agreement; (iii) the defendant’s breach; and (iv) resulting damage to the plaintiff.” *In re Facebook, Inc., Consumer Priv. User Profile Litig.*, 402 F. Supp. 3d 767, 801 (N.D. Cal. 2019) (“*Facebook Consumer Privacy*”). At the motion to dismiss stage, the Court must determine whether Google’s contract with Plaintiffs is “reasonably susceptible” to Plaintiffs’ interpretation. *Id.* at 789. Additionally, “the contract language must be assessed objectively, from the perspective of a

reasonable [Google] user.” *Id.*; *see also Williams v. Apple, Inc.*, No. 19-cv-04700-LHK, 2021 WL 2186223, at *5 (N.D. Cal. May 28, 2021) (“[C]ourts in construing and applying a standardized contract seek to effectuate the reasonable expectations of the average member of the public who accepts it.” (quoting Restatement (Second) of Contracts § 211(2))).

Plaintiffs allege that their relationship with Google was governed by a contract consisting of the “Google Terms of Service, the Google Chrome and Chrome OS Additional Terms of Service, and the Chrome Privacy Notice.” SAC ¶ 268. Additionally, Plaintiffs allege that this contract incorporated at least three additional documents—Google’s Privacy Policy, the “Search & Browse Privately” page, and the Incognito Splash Screen—such that these additional documents are part of the contract as well. *Id.*

According to Plaintiffs, the Chrome Privacy Notice, Google’s Privacy Policy, the “Search & Browse Privately” page, and the Incognito Splash Screen promised that, if Plaintiffs visited websites in “private browsing mode,” Google would not collect Plaintiffs’ data. *Id.* ¶¶ 269–272. Thus, because Google collected Plaintiffs’ data when Plaintiffs were using “private browsing mode,” Google breached this promise. *Id.* Plaintiffs further allege that they “fulfilled their obligations under the relevant contracts,” that “Google was able to obtain the personal property of Plaintiffs,” and that Plaintiffs “did not receive the benefit of the bargain for which they contracted.” *Id.* ¶¶ 273–75.

Google concedes that the Chrome Privacy Notice governed, and continues to govern, Google’s relationship with Plaintiffs. *See* Mot. at 13–16. Google also concedes that the Privacy Policy and “Search & Browse Privately” page governed Google’s relationship with Plaintiffs until March 31, 2020. *See id.* at 10–13.

However, Google argues that, because the Incognito Splash Screen was never part of Google’s contract with Plaintiffs, Plaintiffs’ breach of contract claim may not rely on the Incognito Splash Screen. *See id.* at 5–7. Additionally, Google argues that, because Google’s Privacy Policy ceased being part of Google’s contract with Plaintiffs on March 31, 2020, Plaintiffs “should not be permitted to state a contract claim based on the Privacy Policy after March 31,

2020.” *Id.* at 10. Finally, Google argues that the Incognito Splash Screen, Google’s Privacy Policy, the “Search & Browse Privately” page, and the Chrome Privacy Notice do not contain promises regarding Google’s collection of Plaintiffs’ data. *See* Mot. at 7–15. The Court discusses these arguments in turn.

1. A Reasonable User Could Read Google’s Contract with Plaintiffs as Incorporating the Incognito Splash Screen

Google contends that the Incognito Splash Screen is not part of Google’s contract with Plaintiffs because “[n]either the Google Terms of Service, the Google Chrome Terms of Service, the Chrome OS Additional Terms of Service, nor the Chrome Privacy Notice refer to or mention the Incognito Screen.” Mot. at 5. For the reasons below, the Court rejects this contention.

Under California law, a “contract may validly include the provision of a document not physically a part of the basic contract.” *Shaw v. Regents of University of California*, 58 Cal. App. 4th 44, 54 (1997) (quoting *Williams Constr. Co. v. Standard-Pacific Corp.*, 254 Cal. App. 2d 442, 454 (1967)). Indeed, another court in this District has stated that “California law makes it quite easy to incorporate a document by reference.” *See In re Facebook, Inc., Consumer Priv. User Profile Litig.*, 402 F. Supp. 3d 767, 791 (N.D. Cal. 2019) (Chhabria, J.).

Whether parties have “incorporate[d] by reference into their contract the terms of some other document” is a factual inquiry. *Shaw*, 58 Cal. App. 4th at 54. Specifically, “[f]or the terms of another document to be incorporated into the document executed by the parties the reference must be clear and unequivocal, the reference must be called to the attention of the other party and he must consent thereto, and the terms of the incorporated document must be known or easily available to the contracting parties.” *Id.* However, the “contract need not recite that it ‘incorporates’ another document, so long as it ‘guide[s] the reader to the incorporated document.’” *Id.* (quoting *Bakery v. Aubry*, 216 Cal. App. 3d 1259, 1264 (1989)). Accordingly, if a contract “directed” the parties to a document and the parties “received the document,” the document is part of the contract. *See Marchand v. Northrop Grumman*, Case No. 16-cv-06825-BLF, 2017 WL 2633132, at *5 (N.D. Cal. Jun 19, 2017).

Under this standard, a reasonable user could conclude that Plaintiffs' contract with Google incorporated the Incognito Splash Screen. Google's Privacy Policy, which Google concedes was part of the contract, expressly stated in an "Introduction" section that Plaintiffs could "choose to browse the web privately using Chrome in Incognito mode." SAC ¶ 45. Similarly, the Chrome Privacy Notice, which Google concedes was part of the contract, encouraged Plaintiffs to "us[e] incognito mode." See ECF No. 165-22 at 11. The Chrome Privacy Notice also directed Plaintiffs to a page called "Browse in private," which provided directions on how to open Chrome in Incognito Mode. *Id.* Thus, because the Incognito Splash Screen "appear[ed] whenever a user enters Incognito mode," SAC ¶ 52, a reasonable user could read Google's Privacy Policy and the Chrome Privacy Notice as incorporating the Incognito Splash Screen by "guid[ing] the reader to" enter Incognito Mode. See *Shaw*, 58 Cal. App. 4th at 54. Google itself has described the Incognito Splash Screen as "conspicuous" and has stated that the Screen is "presented precisely to ensure users understand what Incognito mode means." See ECF No. 82 at 10; ECF No. 92 at 4.

Judge Chhabria's decision in *Facebook Consumer Privacy*, which found that the 2012 version of Facebook's "Statement of Rights and Responsibilities" ("SRR") incorporated Facebook's "Data Use Policy," is instructive. 402 F. Supp. 3d at 790. The "first section of the SRR, entitled 'Privacy,' call[ed] out the Data Use Policy in the second sentence, provide[d] a link to it, and encourage[d] the user to read it." *Id.* at 791. Additionally, a different section of the SRR told "users to read the Data Use Policy to learn about 'how you can control what information other people may share with applications.'" *Id.*

Although Google's Privacy Policy and the Chrome Privacy Notice do not use the term "Incognito Splash Screen," those documents guided Plaintiffs to the Incognito Splash Screen in the same way that Facebook's SRR guided Facebook users to the Data Use Policy. Specifically, Google's Privacy Policy and the Chrome Privacy Notice encouraged Plaintiffs to use Incognito Mode and provided express instructions on how to do so. See SAC ¶ 45; ECF No. 165-22 at 11. Because the Incognito Splash Screen "appears whenever a user enters Incognito Mode," the combined effect of Google's Privacy Policy and the Chrome Privacy Notice was to "provide[] a

link” to the Incognito Splash Screen and to “encourage the user to read it.” *See Facebook Consumer Privacy*, 402 F. Supp. 3d at 791. Thus, California law “mitigates in favor of the conclusion” that the Incognito Splash Screen was part of Google’s contract with Plaintiffs. *Id.*

Google’s arguments to the contrary are unconvincing. Google argues that, because Google’s Privacy Policy and the Chrome Policy Notice do not expressly “refer to or mention” the Incognito Splash Screen, those documents do not incorporate the Incognito Splash Screen. Mot. at 5. However, California law is clear that the contract need only “guide[,]” *Shaw*, 58 Cal. App. 4th at 54, or “direct,” *Marchand*, 2017 WL 2633132, at *5, the parties to a document in order to incorporate that document. Whatever the precise scope of the terms “guide” and “direct,” the California Supreme Court’s use of those terms means that parties are not required to reference a document by name to incorporate the document. Indeed, California law “makes it quite easy to incorporate a document by reference.” *Facebook Consumer Privacy*, 402 F. Supp. 3d at 790. Thus, the fact that Google’s Privacy Policy and the Chrome Policy Notice do not use the phrase “Incognito Splash Screen” does not alter the Court’s conclusion.

Additionally, although Google relies heavily on *In re Facebook, Inc. Internet Tracking Litigation*, 956 F.3d 589, 610 (9th Cir. 2020) (“*Facebook Internet Tracking*”), that case does not provide Google with any support. Like the plaintiffs in *Facebook Consumer Privacy*, the plaintiffs in *Facebook Internet Tracking* alleged that Facebook’s “Statement of Rights and Responsibilities” (“SRR”) incorporated Facebook’s “Data Use Policy.” 956 F.3d at 610. However, unlike the plaintiffs in *Facebook Consumer Privacy*, 402 F. Supp. 3d at 790, who relied on the 2012 version of the SRR, the plaintiffs in *Facebook Internet Tracking*, 956 F.3d at 610, relied on the April 2011 version of the SRR. The April 2011 version of the SRR contained no references to the Data Use Policy, and instead referred users to an older document called the “Privacy Policy.” *Facebook Internet Tracking*, 956 F.3d at 610 (“Although the [SRR] directs readers to the Privacy Policy, Plaintiffs rely on the latest version of this document, titled ‘Data Use Policy.’”). Indeed, as Judge Chhabria explained in *Facebook Consumer Privacy*, it was not until “mid-2012” that Facebook updated the SRR to reference the “Data Use Policy.” 402 F. Supp. 3d

at 790 n.11. Thus, because the *Facebook Internet Tracking* plaintiffs relied on the April 2011 version of the SRR, which guided users to the “Privacy Policy” instead of the “Data Use Policy,” the Ninth Circuit concluded that the “SRR d[id] not reference a Data Use Policy.” 956 F.3d at 610. That conclusion has no bearing on the instant case.

For all these reasons, a reasonable user could read Google’s contract with Plaintiffs as incorporating the Incognito Splash Screen. Accordingly, the Court need not address Plaintiffs’ alternative argument that, even if the Incognito Splash Screen was not part of the contract, the Screen should be used to interpret the contract. *See* Opp. at 7.

2. A Reasonable User Could Read Google’s Contract with Plaintiffs as Incorporating Google’s Privacy Policy After March 30, 2020

Although Google concedes that Google’s contract with Plaintiffs incorporated Google’s Privacy Policy before March 31, 2020, Google asserts that Google’s Privacy Policy ceased to be part of the contract on March 31, 2020. Mot. at 10. Accordingly, Google contends that Plaintiffs “should not be permitted to state a contract claim based on the Privacy Policy after March 31, 2020.” *Id.* For the reasons below, the Court disagrees.

During the “Class Period,” which Plaintiffs define as “June 1, 2016 through the present,” SAC ¶ 192, there have been three versions of Google’s “Terms of Service.” The first two versions stated: “By using our Services, you agree that Google can use such data in accordance with our privacy policies.” *See* ECF No. 165-17 at 3; ECF No. 165-18 at 2. The current version, which has been in place since March 31, 2020, instead states: “Besides these terms, we also publish a Privacy Policy. Although it’s not part of these terms, we encourage you to read it to better understand how you can update, manage, export, and delete your information.” ECF No. 165-19 at 1.

Relying on this Court’s decision in *Calhoun v. Google LLC*, 526 F. Supp. 3d 605 (N.D. Cal. 2021), Google contends that, because the current version of the Terms of Service states that Google’s Privacy Policy is “not part of these terms,” Google’s Privacy Policy has not been part of Google’s contract with Plaintiffs since March 31, 2020. Mot. at 10. In *Calhoun*, the plaintiffs were “users of Google’s Chrome browser” who “chose not to ‘Sync’ their [Chrome] browsers

1 with their Google accounts while browsing the web.” *Id.* at 613. The *Calhoun* plaintiffs brought
 2 claims against Google alleging that Google had collected the plaintiffs’ data despite Google’s
 3 representation that it would only collect the data of Chrome users who chose to “Sync” their
 4 browsers with their Google Accounts. *See id.* at 613–615. In its motion to dismiss, Google
 5 argued that the *Calhoun* plaintiffs had consented to Google’s data collection by agreeing to
 6 Google’s Privacy Policy, which disclosed the data collection. *Id.* at 621.

7 The Court rejected Google’s consent argument in *Calhoun* because, among other reasons,
 8 Google’s latest Terms of Service “explicitly excluded Google’s Privacy Policy” and thus a
 9 “reasonable user consenting to Google’s Terms of Service on or after March 31, 2020 might have
 10 concluded that she was not consenting to Google’s Privacy Policy.” *Id.* In the instant case,
 11 Google argues that, because the Court concluded that the *Calhoun* plaintiffs were not bound by
 12 Google’s Privacy Policy after March 2020, it would be inconsistent for the Court to conclude that
 13 Google was bound by Google’s Privacy Policy after March 2020. Mot. at 10.

14 However, the Chrome Privacy Notice, which Google concedes is part of the contract,
 15 independently references Google’s Privacy Policy. Specifically, each version of the Chrome
 16 Privacy Notice that has been in effect since March 30, 2020 has stated: “[A]ny personal
 17 information that is provided to Google or stored in your Google Account will be used and
 18 protected in accordance with the Google Privacy Policy.” *See* ECF Nos. 165-21, 165-22, 192-2.

19 Moreover, Google’s Terms of Service instruct Chromes users to follow the Chrome
 20 Privacy Notice in the event that the Terms of Service and the Chrome Privacy Notice conflict with
 21 each other. Specifically, the version of Google’s Terms of Service that has been in effect since
 22 March 30, 2020 states that users must follow “service-specific additional terms” and that, “[i]f the
 23 [Terms of Service] conflict with the service-specific additional terms, the additional terms will
 24 govern for that service.” ECF No. 165-19 at 3, 13.

25 Thus, a reasonable Chrome user could conclude that Google’s Privacy Policy continued to
 26 be part of Google’s contract with Plaintiffs after March 30, 2020. Because the Chrome Privacy
 27 Notice “call[ed] out” Google’s Privacy Policy, “provide[d] a link to it,” and “encourage[d] the

1 user to read it,” a reasonable user could conclude that the Chrome Privacy Notice incorporates
 2 Google’s Privacy Policy. *Facebook Consumer Privacy*, 402 F. Supp. 3d at 791. In turn, because
 3 the Terms of Service direct users to follow “service-specific additional terms” in the event of a
 4 conflict, a reasonable user could conclude that the Chrome Privacy Notice, not the Terms of
 5 Service, is binding with respect to Google’s Privacy Policy. ECF No. 165-19.

6 This conclusion is not inconsistent with *Calhoun*. As discussed, the Court’s task at the
 7 motion to dismiss stage is to determine whether Google’s contract with Plaintiffs is “reasonably
 8 susceptible” to Plaintiffs’ interpretation. *See Facebook Consumer Privacy*, 402 F. Supp. 3d at
 9 789. In *Calhoun*, the Court held that a “reasonable user consenting to Google’s Terms of Service
 10 on or after March 31, 2020 *might have* concluded that she was not consenting to Google’s Privacy
 11 Policy.” *Calhoun*, 526 F. Supp. 3d at 621 (emphasis added). Accordingly, *Calhoun* does not
 12 preclude Plaintiffs’ interpretation, which is that a reasonable user *might have* concluded that
 13 Google’s Privacy Policy continued to be part of the contract after March 31, 2020. Indeed, the
 14 fact that a contract is “reasonably susceptible” to one interpretation does not mean that the contract
 15 is not “reasonably susceptible” to a competing interpretation.

16 Thus, Plaintiffs may rely on the March 31, 2020 version of Google’s Privacy Policy to
 17 support their breach of contract claim.

18 **3. A Reasonable User Could Read the Contract as Promising that “Private Browsing 19 Mode” Would Prevent Google from Collecting Users’ Data**

20 Google also contends that Plaintiffs’ breach of contract claim must be dismissed because
 21 Google did not promise Plaintiffs that using “private browsing mode” would prevent Google from
 22 collecting Plaintiffs’ browsing data. For the reasons below, the Court rejects this contention.

23 Under California law, the “most important[.]” principle of contract interpretation is that the
 24 “‘whole of a contract is to be taken together, so as to give effect to every part, if reasonably
 25 practicable, each clause helping to interpret the other.’” *International Brotherhood of Teamsters*
 26 *v. NASA Services, Inc.*, 957 F.3d 1038, 1042 (9th Cir. 2020). Indeed, California courts have
 27 “consistently reaffirm[ed]” that “‘the intention of the parties is to be collected from the entire
 28

instrument and not detached portions thereof, it being necessary to consider all of the parts to determine the meaning of any particular part as well as of the whole.” *Id.* (quoting *Ajax Magnolia One Corp. v. S. Cal. Edison Co.*, 167 Cal. App. 2d 743, 748 (1959)). “[I]ndividual clauses and particular words must be considered in connection with the rest of the agreement, and all of the writing and every word of it will, if possible, be given effect.” *Id.* (quoting *Ajax*, 167 Cal. App. 2d at 748).

The Court already has determined that a reasonable user could read statements from the Incognito Splash Screen, Google’s Privacy Policy, the “Search & Browse Privately” page, and the Chrome Privacy Notice as promising that “private browsing mode” prevents Google from collecting users’ browsing data. In Google’s motion to dismiss the FAC, Google argued that Plaintiffs “expressly consented to Google’s alleged data collection while they were in private browsing mode.” *Brown*, 525 F. Supp. 3d at 1063. Specifically, Google argued that Plaintiffs “expressly consented to Google’s Terms of Service, which incorporated Google’s Privacy Policy, and Google’s Privacy Policy disclosed that Google would receive the data from its third-party services.” *Id.*; *see also* ECF No. 82 at 10–11. In rejecting this argument, the Court stated that the portion of Google’s Privacy Policy which explains Google’s data collection practices “never mentions private browsing” and does not “explain that Google collects this data from users in private browsing.” *Brown*, 525 F. Supp. 3d at 1064. By contrast, other portions of Google’s Privacy Policy, as well as other Google documents, “present private browsing as a way that users can manage their privacy and omit Google as an entity that can view users’ activity while in private browsing mode.” *Id.* at 1064.

Specifically, in the Court’s order denying Google’s motion to dismiss the FAC, the Court highlighted the following portions of the Incognito Screen, the Privacy Policy, the “Search & Browse privately” page, and the Chrome Privacy Notice:

- The Incognito Splash Screen’s “list of entities that can view a user’s activity in private browsing mode,” which “omits Google” and instead lists: “Websites you visit[;] Your employer or school[;] Your internet service provider.”

- The Incognito Splash Screen’s statement that: “Now you can browse privately, and other people who use this device won’t see your activity.”
- The Incognito Splash Screen’s statement that: “Chrome won’t save . . . [y]our browsing history [or] [c]ookies and site data.”
- The “Search & Browse privately” page’s statement that: “You’re in control of what information you share with Google when you search. To browse the web privately, you can use private browsing.”
- The Chrome Privacy Notice’s statement that: “You can limit the information Chrome stores on your system by using incognito mode or guest mode. In these modes, Chrome won’t store certain information, such as: . . . Basic browsing history information like URLs, cached paged text, or IP addresses of pages linked from the websites you visit [and] Snapshots of pages that you visit.”
- Google’s Privacy Policy’s statement that: “You can . . . choose to browse the web privately using Chrome in Incognito mode. And across our services, you can adjust your privacy settings to control what we collect and how your information is used.”

Id. at 1065–66 (internal quotations and citations omitted). The Court concluded that a reasonable internet user could reach each of these statements as representing that “private browsing mode” prevents Google from collecting users’ data. *Id.*

Given the Court’s previous conclusion regarding each of these individual statements, a reasonable user, reading Google’s contract with Plaintiffs as a whole, could easily conclude that Google promised Plaintiffs that using “private browsing mode” would prevent Google from collecting Plaintiffs’ data. Indeed, even if some of the individual statements in the contract are ambiguous, reading the contract as a whole, with “each clause helping to interpret the other,” clarifies any ambiguities. *International Brotherhood of Teamster*, 957 F.3d at 1042. A reasonable user could conclude that Google’s repeated affirmative assertions that “private browsing mode”

1 provides internet users with “privacy” and “control” were meant to emphasize to users that Google
2 would provide users with the maximum amount of data privacy.

3 Google does not attempt to read the contract as a whole. Instead, Google isolates each
4 provision and attempts to explain why that provision does not support Plaintiffs’ claim. *See* Mot.
5 at 7–15. However, because “the intention of the parties is to be collected from the entire
6 instrument and not detached portions thereof, it being necessary to consider all of the parts to
7 determine the meaning of any particular part as well as of the whole,” Google’s method is
8 misguided. *International Brotherhood of Teamster*, 957 F.3d at 1042 (internal citations omitted).

9 Regardless, the Court previously has rejected almost all of Google’s arguments regarding
10 individual provisions of the contract. For example, Google highlights a statement from Google’s
11 Privacy Policy—“across our services, you can adjust your privacy settings to control what we
12 collect and how your information is used”—and contends that this statement is “too generalized to
13 support [Plaintiffs’] breach of contract claim.” Mot. at 11 (internal citations omitted). However,
14 Google omits the preceding sentence of Google’s Privacy Policy, which states that users can
15 “choose to browse the web privately using Chrome in Incognito mode.” SAC ¶ 45. As the Court
16 previously concluded, a reasonable user could read these two sentences as promising that
17 “Incognito mode [i]s a way that users can control the information that Google collects.” *Brown*,
18 525 F. Supp. 3d at 1066. Google provides no reason for the Court to revisit this conclusion, or its
19 conclusions regarding Google’s other representations.

20 Additionally, although Google argues that contract interpretation principles compel a
21 different interpretation of the Chrome Privacy Notice than the Court previously reached, this
22 argument is unconvincing. The Chrome Privacy Notice states: “You can limit the information
23 Chrome stores on your system by using incognito mode or guest mode. In these modes, Chrome
24 won’t store . . . [b]asic browsing history information like URLs, cached page text, or IP addresses
25 of pages linked from the websites you visit [and] Snapshots of pages that you visit.” ECF No.
26 165-22 at 11. The Court previously concluded that “a reasonable user could read this statement to
27 mean that their browsing history and cookies and site data would not be saved” by Chrome and

that “a user might reasonably associate Chrome with Google because Chrome is Google’s browser.” *Brown*, 525 F. Supp. 3d at 1065–66. Google acknowledges this conclusion. Mot. at 14 n.8. However, Google contends that the Court’s analysis should be different “in the context of a breach of contract analysis.” *Id.* Specifically, Google contends that the “alleged contract separately defines ‘Chrome’ and ‘Google’”; that it is a rule of contract interpretation that “defined terms must be given their defined meaning”; and that because “Chrome” and “Google” are given separate definitions, “Chrome” cannot be read as referring to “Google.” Mot. at 14 (internal citations omitted). This argument ignores that, although “Google” and “Chrome” are not synonymous, Google has complete control over Chrome’s functionality and Google obtains internet users’ data by *causing Chrome to send Google the data*. Accordingly, a reasonable user could read Google’s representations about Chrome to mean that Google designed Chrome not to send Google data while in “private browsing mode.”

Finally, the Court rejects Google’s argument that Plaintiffs’ interpretation improperly relies on subjective intent. Citing Plaintiffs’ allegation that Plaintiffs “‘reasonably expected that Google would not collect their data while in Incognito mode,’” Mot. at 8 (citing SAC ¶ 51), Google contends that “Plaintiffs’ allegations . . . fail to state a contract claim because: ‘It is not the parties’ subjective intent that matters, but rather their objective intent, as evidenced by the words of the contract,’” *id.* (citing *Block v. eBay, Inc.*, 747 F.3d 1135, 1138 (9th Cir. 2014)). Although Google is correct that the contract must be interpreted objectively, the objective meaning of a contract is determined by reading the contract “from the perspective of a reasonable [Google] user.” *See Facebook Consumer Privacy*, 402 F. Supp. 3d at 789. By offering an interpretation about what Plaintiffs “reasonably expected,” Plaintiffs provide that perspective. SAC ¶ 51.

Thus, the Court DENIES Google’s motion to dismiss Plaintiffs’ breach of contract claim.

B. Plaintiffs Have Adequately Stated a UCL Claim Based on Google’s Data Collection Practice

The California Unfair Competition Law (“UCL”) provides a cause of action against persons who engage in “unfair competition,” which includes business practices that are “(1)

unlawful, (2) unfair, or (3) fraudulent.” *Backhaut v. Apple, Inc.*, 74 F. Supp. 3d 1033, 1050 (N.D. Cal. 2014) (citing Cal. Bus. & Prof. Code § 17200). This cause of action is available to any “person who has suffered injury in fact and has lost money or property as a result of the unfair competition.” Cal. Bus. & Prof. Code § 17204.

Plaintiffs allege that Google’s business practice of collecting Plaintiffs’ data while Plaintiffs were using “private browsing mode” was “unlawful” and “unfair” because it constituted a “violation of the Federal Wiretap Act, 18 U.S.C. § 2510, *et seq.*; the California Invasion of Privacy Act, Cal. Penal Code §§ 631 and 632; the California Computer Data Access and Fraud Act, Cal. Penal Code § 502, *eq seq.*; Invasion of Privacy; Intrusion Upon Seclusion; Breach of Contract; and California Business & Professions Code § 22576.” SAC ¶¶ 279, 281. Plaintiffs further allege that they “have suffered injury-in-fact, including the loss of money and/or property as a result of . . . the unauthorized disclosure and taking of their personal information which has value as demonstrated by its use and sale by Google.” *Id.* ¶ 282. Specifically, Plaintiffs “have suffered harm in the form of diminution of the value of their private and personally identifiable data and content.” *Id.*

Google argues that Plaintiffs’ UCL claim should be dismissed for two reasons and argues that, even if Plaintiffs’ UCL claim is not dismissed, Plaintiffs should be limited to seeking injunctive relief. First, Google contends that the UCL claim should be dismissed because Plaintiffs have not “plausibly alleged that they ‘lost money or property’ as a result of Google’s conduct.” Mot. at 16 (quoting Cal. Bus. & Prof. Code § 17204). Second, Google contends that the UCL claim should be dismissed because Plaintiffs have not adequately alleged that they relied on Google’s statements. Mot. at 24. Finally, Google contends that Plaintiffs should be limited to injunctive relief because Plaintiffs “do not allege that Google took any money from them.” Mot. at 23. The Court addresses each contention in turn.

1. Plaintiffs Have Plausibly Alleged that Google’s Data Collection Practice Caused Plaintiffs to Lose “Money or Property”

As noted, Plaintiffs must show that they “ha[ve] suffered injury in fact and ha[ve] lost

1 money or property as a result of the unfair competition.” Cal. Bus. & Prof. Code § 17204.

2 Google argues that, because Plaintiffs’ data is not “property” and because Plaintiffs did not pay to
3 use “private browsing mode,” Google’s practice of collecting Plaintiffs’ data when Plaintiffs used
4 “private browsing mode” cannot have caused Plaintiffs to lose “money or property.” Mot. at 17–
5 23. For the reasons below, the Court rejects Google’s argument.

6 The California Supreme Court has explained that the phrase “[i]njury in fact” is a legal
7 term of art” that comes from the “requirements for federal standing under [A]rticle III, section 2 of
8 the United States Constitution.” *Kwikset Corp. v. Superior Court*, 51 Cal. 4th 310, 322 (2011).
9 “Under federal law, injury in fact is ‘an invasion of legally protected interest which is (a) concrete
10 and particularized; and (b) actual or imminent, not conjectural or hypothetical.’” *Id.* (quoting
11 *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992)). The UCL “incorporate[s] the
12 established federal meaning” of “injury in fact.” *Id.*

13 To show that they have “lost money or property,” Plaintiffs “must demonstrate some form
14 of economic injury,” which “is itself a classic form of injury in fact.” *Id.* at 323. Thus, because
15 federal standing “may be predicated on a broader range of injuries,” the effect of the “lost money
16 or property” requirement is to “render[] standing under [the UCL] substantially narrower than
17 federal standing.” *Id.* at 324.

18 However, the California Supreme Court has held that “[t]here are innumerable ways in
19 which economic injury from unfair competition may be shown.” *Id.* at 323. For example, a
20 “plaintiff may (1) surrender in a transaction more, or acquire in a transaction less, than he or she
21 otherwise would have; (2) have a present or future property interest diminished; (3) be deprived of
22 money or property to which he or she has a cognizable claim; or (4) be required to enter into a
23 transaction, costing money or property, that would otherwise have been unnecessary.” *Id.*

24 Plaintiffs allege that the “cash value” of the data which Google collected “can be
25 quantified” and that there is an active market for such data. *See* SAC ¶¶ 123, 127. For example, a
26 recent study found that internet users are willing to pay up to \$52.00/year to keep their browsing
27 histories private. *Id.* ¶ 128. Google itself has set up a project called “Google Screenwise Trends”

which pays internet users “up to \$3 per week” to “add a browser extension that shares with Google the sites they visit and how they use them.” *Id.* ¶ 129–30. Indeed, “a number of platforms have appeared where consumers can and do directly monetize their own data.” *Id.* ¶ 135. For example, a company called Brave now offers a web browser which “will pay users to watch online targeted ads, while blocking out everything else.” *Id.* Several other companies, including a company called Killi, have launched exchange platforms that allow individuals to sell their data to third-party applications and websites. *See id.*

These detailed allegations establish at least two cognizable theories of economic injury. First, because Google previously has paid individuals for browsing histories, it is plausible that, had Plaintiffs been aware of Google’s data collection, they would have demanded payment for their data. Thus, by inducing Plaintiffs to give Google their data without payment, Google caused Plaintiffs to “acquire in a transaction less[] than [they] otherwise would have.” *Kwikset*, 51 Cal. 4th at 324. Second, because there are several browsers and platforms willing to pay individuals for data, it is plausible that Plaintiffs will decide to sell their data at some point. Indeed, each named Plaintiff has alleged that he or she is aware of these browsers and platforms. *See SAC* ¶¶ 170, 175, 180, 185, 190. Accordingly, by obtaining Plaintiffs’ data and selling it to advertisers, Google “diminished” Plaintiffs’ “future property interest.” *Kwikset*, 51 Cal. 4th at 324.

Indeed, in *Calhoun*, this Court found economic injury in almost identical circumstances. As discussed, the *Calhoun* plaintiffs were “users of Google’s Chrome browser” who “chose not to ‘Sync’ their [Chrome] browsers with their Google accounts while browsing the web.” *Id.* at 613. The plaintiffs brought a UCL claim against Google based on an allegation that Google had collected the plaintiffs’ data despite Google’s representation that it would only collect the data of Chrome users who chose to “Sync” their browsers. *See id.* at 613–615, 636.

The Court rejected Google’s argument that the *Calhoun* plaintiffs “lack[ed] statutory standing under the UCL because they fail[ed] to allege that Google caused them to lose ‘money or property.’” *Id.* (internal citations omitted). The Court explained that the “Ninth Circuit and a number of district courts, including this Court, have concluded that plaintiffs who suffered a loss

of their personal information suffered economic injury and had standing.” *See id.*; *see also In re Marriott Int’l, Inc., Cust. Data Sec. Breach Litig.*, 440 F. Supp. 3d 447, 461 (D. Md. 2020) (“[T]he growing trend across courts that have considered this issue is to recognize the lost property value of this information.”); *In re Yahoo! Inc. Cust. Data Sec. Breach Litig.*, 2017 WL 3727318, at *13 (N.D. Cal. Aug. 30, 2017) (holding that plaintiffs had adequately alleged injury in fact based on the loss of value of their personal information); *In re Anthem Inc. Data Breach Litig.*, 2016 WL 3029783, at *14 (N.D. Cal. May 17, 2016) (concluding that the plaintiffs had plausibly alleged injury from the loss of value of their personal information).

Although Google acknowledges *Calhoun*, Google asks the Court to reconsider that decision. Mot. at 16. Specifically, Google argues that data does not fit the UCL’s definition of “property,” that *Calhoun* improperly relied on cases addressing Article III standing, and that *Calhoun* improperly relied on cases in which the plaintiffs had paid money to the defendants. *See* Mot. at 17–21. The Court sees no reason to revisit *Calhoun*. Regardless, the Court addresses Google’s primary arguments below.

As an initial matter, Google’s argument that data does not fit within the UCL’s definition of “property” ignores the California Supreme Court’s guidance that a UCL claim may be based on any kind of “economic injury.” Google cites the Ninth Circuit’s three-part test for determining “whether an intangible property rights exists”: “‘First there must be an interest capable of precise definition; second, it must be capable of exclusive possession or control; and third, the putative owner must have established a legitimate claim to exclusivity.’” Mot. at 17 (quoting *Kremen v. Cohen*, 337 F.3d 1024, 1030 (9th Cir. 2003)). Google contends that an internet user’s data does not satisfy this test because data is “not capable of ‘exclusive possession or control’ by the user.” *Id.* However, the California Supreme Court has explained that the UCL only requires a plaintiff to “demonstrate some form of economic injury” and that there are “innumerable ways in which economic injury from unfair competition may be shown.” *Kwikset*, 51 Cal. 4th at 323. As discussed, Plaintiffs have plausibly alleged that Google’s conduct caused Plaintiffs to “acquire in a transaction less[] than [they] otherwise would have” and have “diminished” Plaintiffs’ “future

property interest.” *Id.* at 324. These injuries fall well within the categories of economic injury recognized by the California Supreme Court. *Id.* Thus, the Court need not determine whether data constitutes property under the UCL.

Next, in arguing that cases discussing Article III standing are irrelevant, Google misreads governing precedent. Citing *Cottle v. Plaid Inc.*, Case No. 20-cv-3056-DMR, 2021 WL 1721177 (N.D. Cal. Apr. 30, 2021), which disagreed with *Calhoun*, Google contends that *Calhoun* was wrongly decided because “*Calhoun* ‘rests on four cases that address Article III standing, which is different from UCL standing.’” Mot. at 20 (quoting *Cottle*, 2021 WL 1721177, at *14 n.8). Additionally, Google quotes the California Supreme Court’s statement that UCL standing is “‘substantially narrower than federal standing under [A]rticle III.’” *Id.* at 20–21 (citing *Kwikset*, 51 Cal. 4th at 324). Both Google and *Cottle* misread the California Supreme Court’s precedent. As discussed, UCL standing is narrower than Article III standing because Article III standing “may be predicated on a broader range of injuries” than UCL standing. *Kwikset*, 51 Cal. 4th at 324. However, the “economic injury” required by the UCL is a “classic form of injury in fact” under Article III and there is no precedent which suggests that “economic injury” has a different meaning in the UCL context than it does in the Article III context. *Id.* at 323. Indeed, the Ninth Circuit has stated that the “UCL’s ‘economic injury-in-fact requirement . . . demands no more than the corresponding requirement under Article III of the U.S. Constitution.’” *Reid v. Johnson & Johnson*, 780 F.3d 952, 958 (9th Cir. 2015) (emphasis added). Thus, cases discussing economic injury in the context of Article III have full application to a court’s analysis of UCL standing.

Finally, although Google points out that the cases cited in *Calhoun* involved plaintiffs that had paid the defendants money, Google fails to explain why this difference is significant. For example, Google points out that the plaintiffs in *Marriott* alleged that, but for Marriott’s conduct, “‘they would not have stayed at a Marriott Property, purchased products or services at a Marriott Property, and/or would have paid less.’” Mot. at 21 (citing *Marriott*, 440 F. Supp. 3d at 492). Similarly, Google highlights that, in *Anthem*, “[e]ach California Plaintiff state[d] they *paid* money for health insurance premiums, which were used to pay for services offered by Defendants.” *Id.*

at 22 (quoting *Anthem*, 2016 WL 3029783, at *30 (emphasis added)). Google contends that, because Plaintiffs do not allege that they paid to use “private browsing mode,” *Marriott* and *Anthem* are not relevant to the instant case. Mot. at 21. However, as discussed, the California Supreme Court has stated that a plaintiff has suffered economic injury if the plaintiff “acquire[d] in a transaction less . . . than he or she otherwise would have.” *Kwikset*, 51 Cal. 4th at 324. Under this standard, a party who has provided goods or services in a transaction and has not been paid the fair value of those goods or services has suffered an economic injury even though the party has received money instead of paying money. *Id.* The same logic would apply to parties like Plaintiffs, who have provided valuable data to Google and have received *no* money in return. Thus, the fact that *Marriott* and *Anthem* involved plaintiffs who paid too much money for goods and services does not diminish their general conclusion that “plaintiffs who suffered a loss of their personal information suffered economic injury.” *Calhoun*, 526 F. Supp. 3d at 636.

Thus, Plaintiffs have adequately alleged that they “lost money or property as a result of the unfair competition.” Cal. Bus. & Prof. Code § 17204.

2. Google Fails to Explain Why Plaintiffs Were Required to Allege Reliance

Google also contends that Plaintiffs’ UCL claim must be dismissed because Plaintiffs failed to allege reliance. Mot. at 24. For the reasons below, the Court rejects this argument.

Under California law, “a plaintiff ‘proceeding on a claim of misrepresentation as the basis of his or her UCL action must demonstrate actual reliance on the allegedly deceptive or misleading statements, in accordance with well-settled principles regarding the element of reliance in ordinary fraud actions.’” *Kwikset*, 51 Cal. 4th at 326 (quoting *In re Tobacco II Cases*, 46 Cal. 4th 298, 306 (2009)). Accordingly, plaintiffs that bring UCL claims based on alleged misrepresentations must “specif[y] which statements any of them saw or relied on.” *Ahern v. Apple Inc.*, 411 F. Supp. 3d 541, 564 (N.D. Cal. 2019).

Plaintiffs have not alleged that their UCL claim relies on misrepresentations or omissions. Plaintiffs allege only that their UCL claim is based on Google’s “violation of the Federal Wiretap Act, 18 U.S.C. § 2510, *et seq.*; the California Invasion of Privacy Act, Cal. Penal Code §§ 631 and

632; the California Computer Data Access and Fraud Act, Cal. Penal Code § 502, *eq seq.*; Invasion of Privacy; Intrusion Upon Seclusion; Breach of Contract; and California Business & Professions Code § 22576.” SAC ¶¶ 279, 281.

Moreover, Google provides no legal or factual support for its conclusory argument that an allegation of reliance is required for Plaintiffs’ UCL claim. Indeed, Google’s only argument on this issue is a summary assertion in its reply brief that “[a]ll of Plaintiffs’ claims indisputably are based on Google’s alleged ‘misrepresentation[s] or omission[s]’ in the Incognito Screen and other disclosures.” Reply at 15.

However, as one example, the Wiretap Act, as amended by the Electronic Communications Privacy Act (“ECPA”), generally prohibits the interception of “wire, oral, or electronic communications” and makes no mention of fraud, misrepresentation, or reliance. 18 U.S.C. § 2511(1). Thus, on this record, the Court cannot conclude that Plaintiffs were required to allege reliance. *Kwikset*, 51 Cal. 4th at 326. Accordingly, the Court DENIES Google’s motion to dismiss Plaintiffs’ UCL claim.

3. Plaintiffs May Seek Restitution

Google contends that Plaintiffs may not seek damages for their UCL claim because “Plaintiffs do not allege that Google took any money from them” and do not “identify any ‘property’ that could be ‘returned’ to them.” Mot. at 23. Accordingly, Google contends, “Plaintiffs seek only nonrestitutionary disgorgement,” which is ‘not available’ under the UCL.” *Id.* (quoting *Madrid v. Perot Sys. Corp.*, 130 Cal. App. 4th 440, 460–62 (2005)).

The Court agrees with Google that Plaintiffs may not seek disgorgement as a remedy. *See Korea Supply Co. v. Lockheed Martin Corp.*, 29 Cal. 4th 1134, 1148 (2003) (holding that “nonrestitutionary disgorgement of profits is not an available remedy” under the UCL). However, the Court cannot conclude at this stage that Plaintiff does not have a cognizable theory of restitution. Indeed, Plaintiffs have alleged that Google’s conduct caused a “diminution of the value of [Plaintiffs’] private and personally identifiable data and content.” SAC ¶ 282. Google fails to explain why, if Plaintiffs can quantify this diminution in value, Plaintiffs would not be

entitled to restitution.

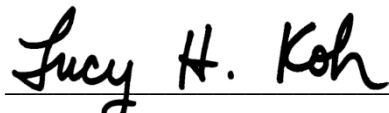
Thus, as in *Calhoun*, the “only monetary remedy Plaintiffs may seek is restitution.”
Calhoun, 526 F. Supp. 3d at 637.

V. CONCLUSION

For the foregoing reasons, the Court DENIES Google’s motion to dismiss.

IT IS SO ORDERED.

Dated: December 22, 2021



LUCY H. KOH
United States District Judge

United States District Court
Northern District of California